sāflink® CORPORATION

PROTECTING YOUR ENTERPRISE THROUGH SECURE AUTHENTICATION™

sāf
COMPUTER NETWORKS
PHYSICAL FACILITIES
APPLICATIONS
MANUFACTURING AUTOMATION SYSTEMS
TIME & ATTENDANCE SYSTEMS
IDENTITY ASSURANCE MANAGEMENT™

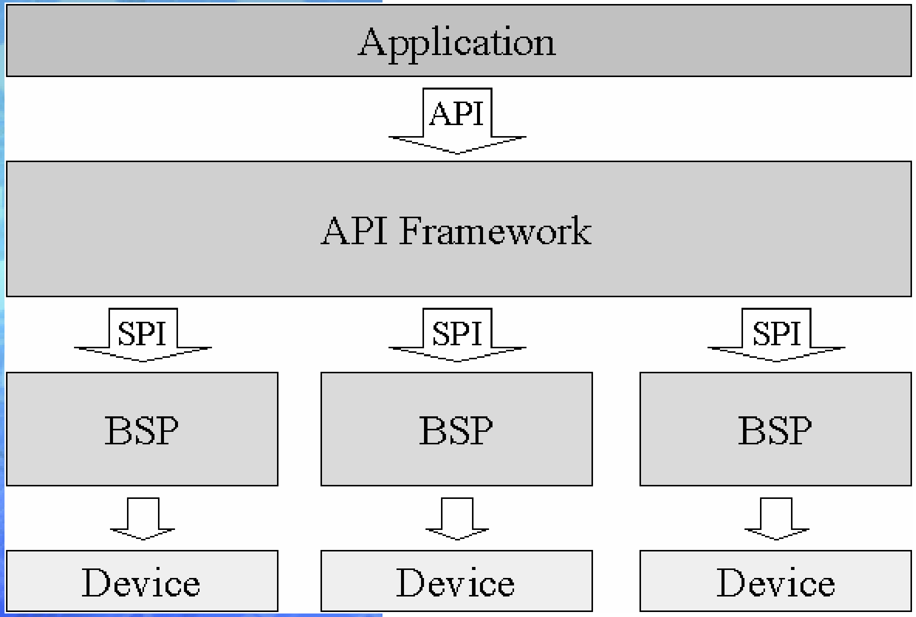
Security Architectures & BioAPI

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Workshop on Biometrics and Remote E-Authentication Over Open Networks

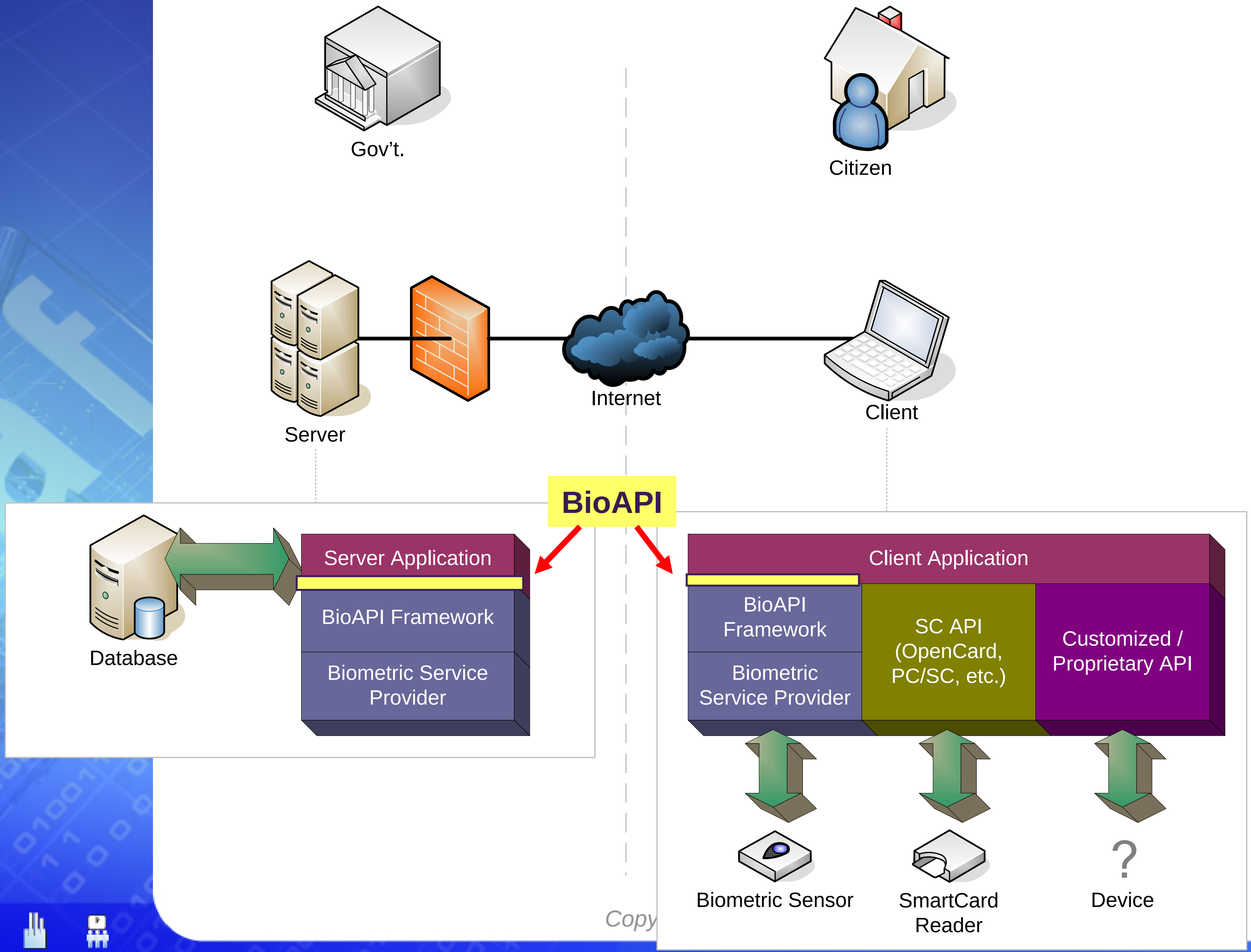
BioAPI Purpose

- ANSI INCITS 358-2002, The BioAPI Specification, defines an open system standard application program interface (API) that allows software applications to communicate with a broad range of biometric technologies in a common way.



- ✓ Simple application interfaces,
- ✓ Standard access methods to biometric functions, algorithms, and devices,
- ✓ Robust biometric data management and storage,
- ✓ Standard methods of managing biometric data and technology types, and
- ✓ Support for biometric verification and identification in distributed computing environments.

Location in Architecture



Security Philosophy

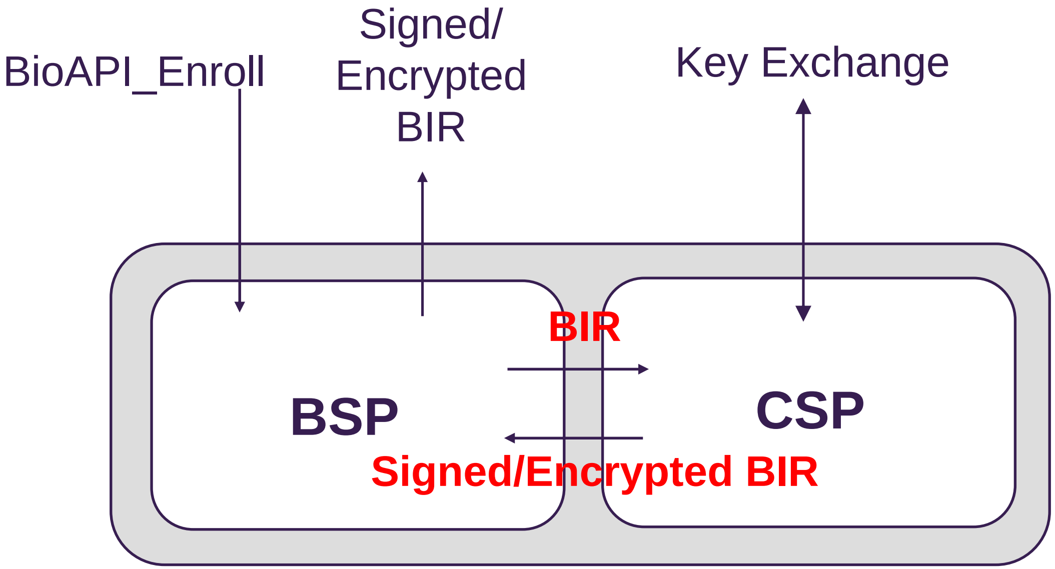
- Support strong security – not mandate it
  - Support use in a wide variety of environments
  - Allow flexibility in choices of security levels and mechanisms
- Biometric API, not a:
  - Authentication API
  - Crypto API
  - Security API
- Use existing security services wherever possible
  - e.g. PKCS-11, CAPI, …
- Many security features can be implemented above the API (application level) or below the API (BSP/device level)

Security Features

- Biometric Identification Record (BIR) - CBEFF
  - Biometric Data Block may be encrypted
  - Entire BIR may be signed
  - Header field indicates security options
  - NOTE: Implies external key management
- Provision for the return of ‘coarsely quantized’ (i.e., incremental) scores
  - Protection against hillclimbing attack
- No linkage of personal identifier/data
  - UUID used as index
- Payload feature
  - Biometrically released secrets
- Support for “self-contained devices”
- 2.0 includes time-stamp/expiration date in header (as well as type) & expanded security block

Architectual Options

- Combined BSP/CSP
  - Biometric functions accessed via BioAPI
  - Cryptographic functions accessed via crypto API
    - e.g., key exchange
  - Ability for BSP to sign/encrypt BIRs



Architectural Options (cont'd)

- BSP may implement Match-on-Card
- BSP functionality may be implemented in hardware device
  - Peripheral, token, smartcard
  - Device may be certified
    - e.g., FIPS 140, Common Criteria
- BSP component may be signed
- BSP may implement
  - Anti-spoofing countermeasures
    - Including liveness detection
  - BSP-controlled BIR database protection
    - DB may be a smartcard
  - Device interface protection

Architectural Options (cont'd)

- Application responsible for:
  - Client/server communications
    - BIP alternative
  - Account database protection
  - End-to-end data security to prevent
    - man in the middle attacks
    - data insertion attacks
    - replay attacks
  - May create debugger hostile environment

The End

Catherine J. Tilton
SAFLINK Corp.
1875 Campus Commons Dr, Suite 301
Reston, VA 20191

ctilton@saflink.com
703-547-0404
Cell 703-472-5546
Fax 703-547-0399